An Integrated Solution for Secure Group Communication in WAN

Olivier Chevassut (OChevassut@lbl.gov)

Ernest Orlando Lawrence Berkeley National Laboratory

Université Catholique de Louvain

D. Agarwal, M. R. Thompson

Ernest Orlando Lawrence Berkeley National Laboratory

G. Tsudik

University of California, Irvine

Outline

- Introduction
- Goals
- Reliable group communication
- Why secure and reliable group communication is hard ?
- Secure and reliable group communication
- Experimental results with a prototype implementation
- Conclusion

Introduction

- Use of the Internet for group communication has increased tremendously
- Security is becoming more important
  - — protection from hackers
  - — privacy of data
  - — avoid a single point of failure (KDC)
- Provide distributed security
- Support
  - — distributed applications
  - — collaborative tools
  - — replicated servers

Goals

- Provide reliable communication for collaborating groups spread across the Internet
  - — simplify distributed application development
  - — simplify communication between components in distributed applications
  - — support flexible delivery capabilities to support a broad range of application needs (e.g., ordering)
- Provide a secure channel among the group members with security services similar to SSL
  - — support confidentiality, authenticity, integrity
  - — support access control based on membership authorization (individually enforced)
  - — security services optional

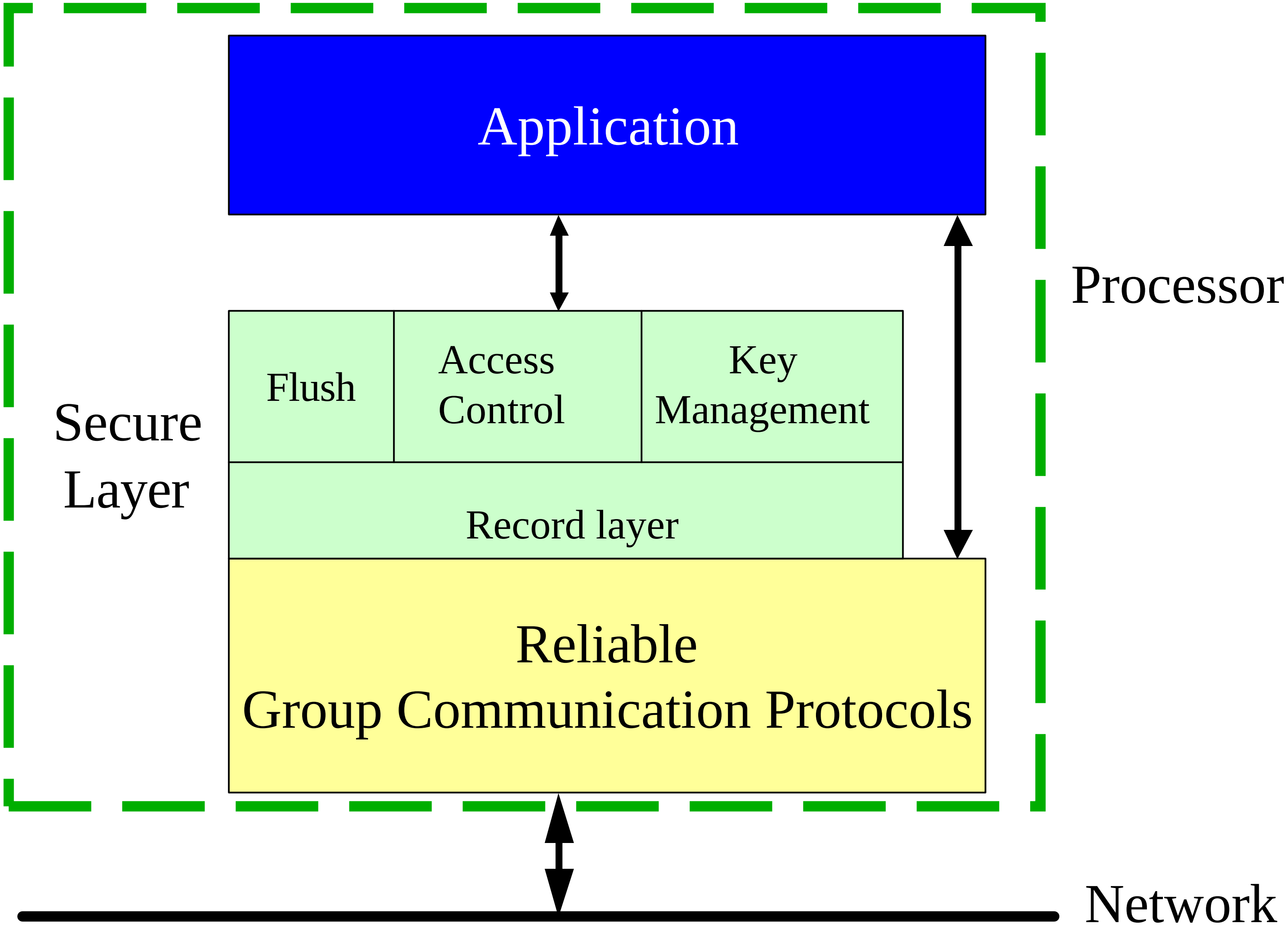
Reliable Group Communication Protocols

- Any member of the group can send messages to the group
- Membership tracked with notification of membership changes
- Deliver messages at each member of the group in a consistent order
  - — FIFO order, causal order, or total order
  - — membership changes delivered in order
  - — virtual synchrony and extended virtual synchrony
    (membership messages ordered with respect to data messages)
- Examples of systems: Isis, Totem, Ensemble, InterGroup

Why Secure and Reliable Group Communication is hard ?

- Dynamic peer groups
  - relatively small (100s of members)
  - no hierarchy and no permanent centralized server
  - frequent membership changes
- Integrate distributed key management with group communication system
- Enable decentralized definition of authorization/ access control policies
- Enforce the policies as part of the key management
- Investigate group certification: how to issue, manage and revoke members’ credentials

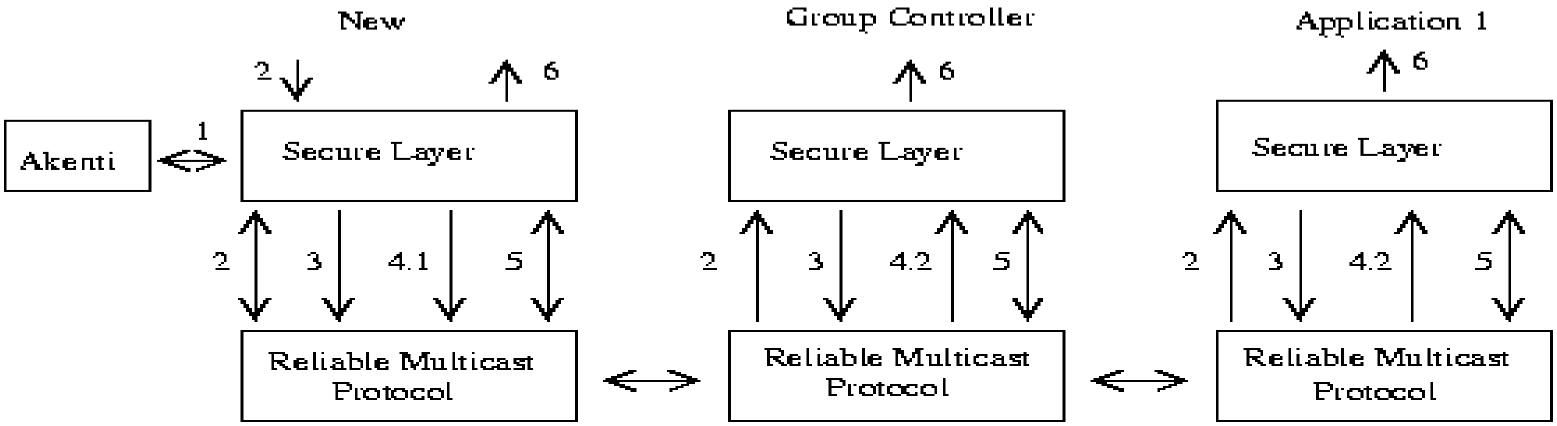
Secure and Reliable Group Communication Architecture



Security Components

- The key management is a group Diffie-Hellman key exchange protocol (Cliques toolkit)
  - — a floating GC initiates the key exchange upon each (authorized) membership change
  - — handle network partitioning and merging
- The access control protocol is based on user's credentials issued by an authorization server (Akenti)
  - — collect policies and uses them to issue users' membership certificates
  - — manage membership certificates (CRL)
- The flush protocol delineates membership in such way that a session key corresponds to a specific membership change

Security Layer on an example: a new users joins the group



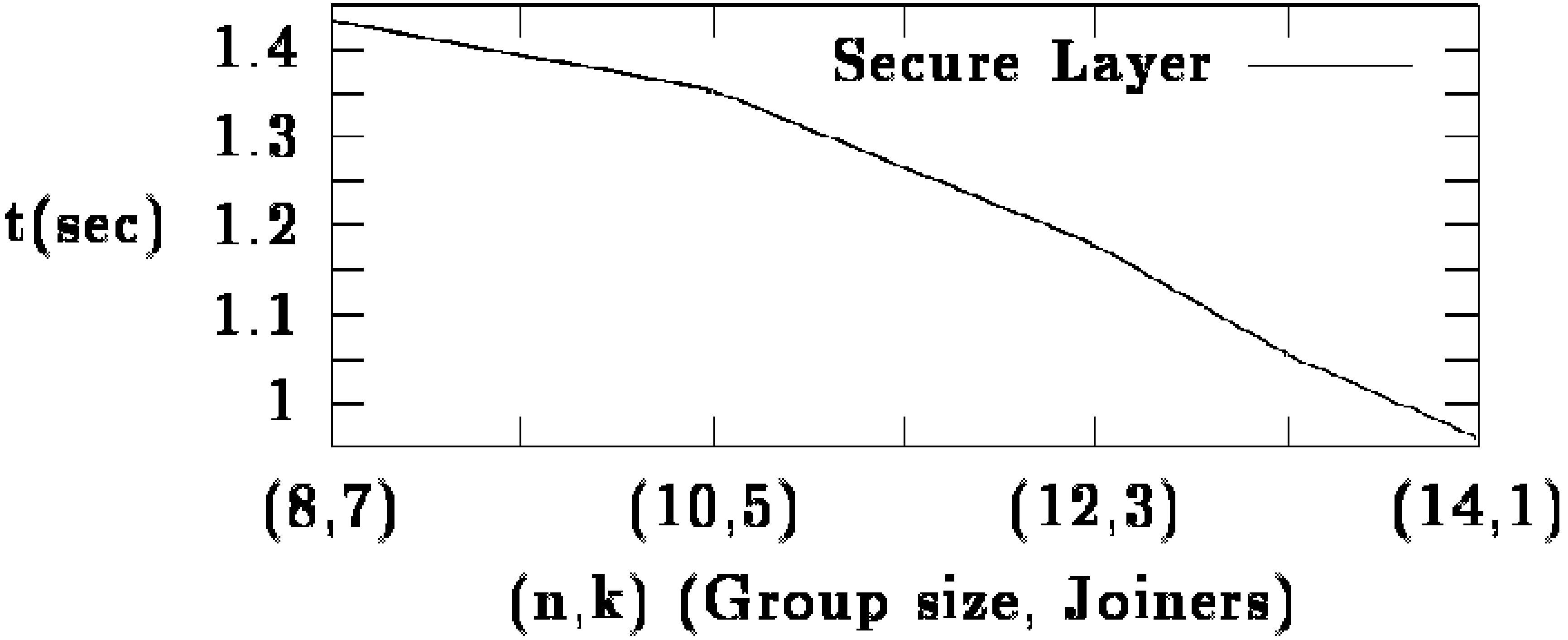
1. **Authorization:** New user gets its membership certificate from Akenti to gain entry into key exchange
2. **Join multicast group**: New user submit a join request and gets back a membership change
3. **Flush:** Secure Layer broadcasts flush msg to indicate end of previous membership
4. **Access control**:
    4.1 New user broadcasts its membership certificate
    4.2 GC checks user's permission and, if authorized, initiates key exchange
5. **Key exchange**: GC, members establish a shared session key
6. **Deliver secure membership**: Secure Layer delivers secure membership to the application

Prototype Implementation

- Written in C
- Implementation intended to be portable
- Akenti provides authorization server
- Totem system provides reliable multicast layer
- Intend to have SSL security model

Experimental Results

- Performance of SL on a group merge with variable-size merging components.The main group size is constant at 15 members. (The cost of the flush is not included).



Conclusion and Further Work

- Threat model of Secure Layer
  - — Protect against eavesdropping and spoofing
  - — Denial of service still a problem (as with SSL) !!

- Current and on-going work
  - — rigorous security analysis
  - — interface definitions
  - — porting Secure Layer to work with InterGroup
    (exhibit prototype at SC'01)
  - — robustness and efficiency improvements